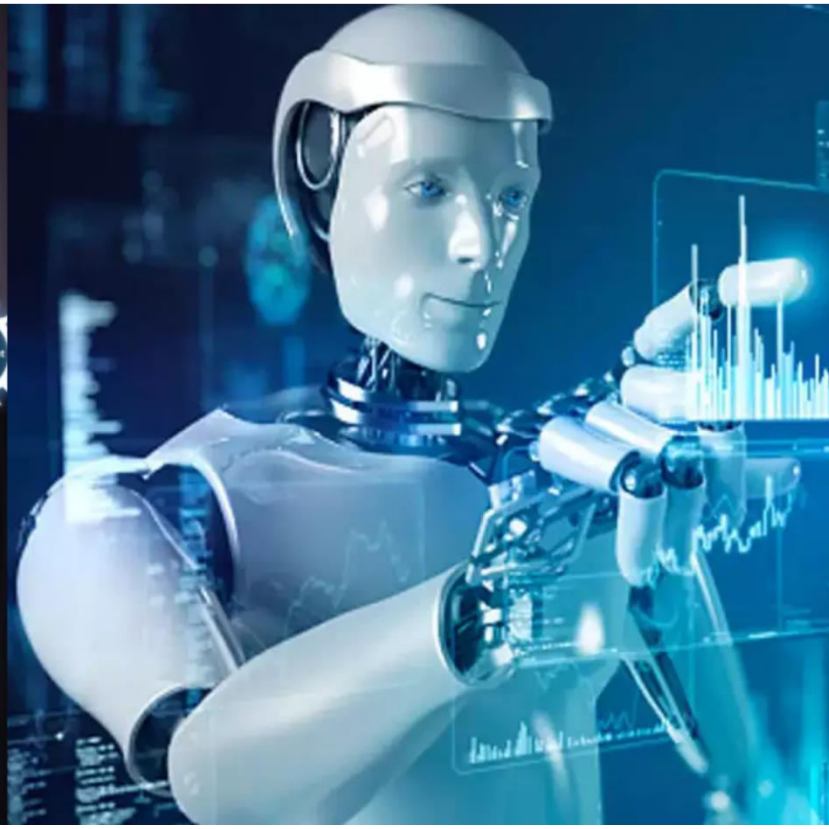
IJIRSET
International Journal of Innovative Research in Science | Engineering | Technology

ISSN(O): 2319-8753
ISSN(P): 2347-6710

International Journal of Innovative Research in Science Engineering and Technology (IJIRSET)

(A Monthly, Peer Reviewed, Refereed, Scholarly Indexed, Open Access Journal)



Impact Factor: 8.699

Volume 15, Issue 3, March 2026

International Journal of Innovative Research of Science, Engineering and Technology (IJIRSET)

Impact Factor 8.699

|www.ijirset.com |A Monthly, Peer Reviewed & Refereed Journal| e-ISSN: 2319-8753| p-ISSN: 2347-6710|

Volume 15, Issue 3, March 2026

|DOI: 10.15680/IJIRSET.2026.1503094|

The Biometric Fortress: A Multi-Layered Framework for Securing Electronic Health Records Through Advanced Cybersecurity and Authentication Mechanisms

Dr. M. Senthilkumar [1], Sajitha.N [2], Sandhiya.R [3], Vinothini.N [4]

Professor, Department of Artificial Intelligence and Data Science, Kongunadu College of Engineering and Technology, Trichy, India[1]

Department of Artificial Intelligence and Data Science, Kongunadu College of Engineering and Technology, Trichy, India[2,3,4]

ABSTRACT: The rapid digitization of healthcare systems has improved the efficiency of patient care, diagnosis, and data management. However, the widespread use of Electronic Health Records (EHRs) has introduced serious cybersecurity challenges in protecting sensitive patient information. Healthcare data such as patient demographics, medical history, diagnostic reports, prescriptions, and insurance details are highly confidential and vulnerable to cyber threats including data breaches, unauthorized access, ransomware attacks, and identity theft. This project focuses on enhancing healthcare data security by integrating cybersecurity mechanisms with biometric authentication techniques. Biometric-based security ensures that only authorized healthcare professionals can access patient data, reducing the risks associated with traditional password-based systems. Biometric traits such as facial recognition and iris patterns provide a reliable method for user authentication. The proposed system emphasizes secure data storage, controlled access, and real-time monitoring to maintain data confidentiality, integrity, and availability. By combining biometric authentication with encryption and access control policies, the system improves trust, regulatory compliance, and overall data safety in digital healthcare environments. Through comprehensive analysis of recent advances—including revocable biometric systems, blockchain integration, multi-factor authentication frameworks, and quantum-resistant cryptography—this paper demonstrates that a multi-layered, adaptive approach to biometric security offers the most robust protection for modern healthcare ecosystems.

KEYWORDS: Healthcare Data Security, Patient Information, Cybersecurity, Biometric Authentication, Electronic Health Records, Multi-Factor Authentication, Blockchain, Revocable Biometrics, Quantum-Safe Cryptography, Internet of Healthcare Things (IoHT).

I. INTRODUCTION

The healthcare sector has experienced a significant digital shift over the last ten years. Electronic Health Records (EHRs) have become the norm, replacing paper records, telemedicine services have improved access to care, and Internet of Things (IoT) devices allow for constant patient monitoring.

While these technological innovations have certainly enhanced the delivery of healthcare by improving diagnostic capabilities, administrative tasks, and personalized treatment plans, they have also introduced an attack surface of unprecedented proportions to cybercriminals.

Healthcare data has a distinct black market value. Unlike financial information, which can be updated after a hack, healthcare data is permanent and replete with personally identifiable information (PII): social security numbers, insurance information, genetic data, and complete medical histories. An EHR can sell for 10 to 50 times the price of a credit card number on the dark web. As a result, healthcare organizations have become the target of choice for cyberattacks such as ransomware, data breaches, and identity theft [1].

International Journal of Innovative Research of Science, Engineering and Technology (IJIRSET)

Impact Factor 8.699

|www.ijirset.com |A Monthly, Peer Reviewed & Refereed Journal| e-ISSN: 2319-8753| p-ISSN: 2347-6710|

Volume 15, Issue 3, March 2026

|DOI: 10.15680/IJIRSET.2026.1503094|

Traditional security methods, namely password authentication, have been grossly insufficient in this context. Passwords are susceptible to phishing, brute-force attacks, and credential stuffing. Furthermore, in medical environments where timely access to patient data may be a matter of life and death, complex password requirements can create workflow bottlenecks, causing medical professionals to resort to insecure practices like password sharing or writing passwords on sticky notes. The underlying issue is that passwords rely on "something you know," which can be phished, brute-forced, or socially engineered [2][3].

Biometric authentication provides a compelling solution by relying on "something you are" – distinct physiological or behavioral traits that are intrinsically linked to an individual and extremely hard to replicate or steal. Fingerprints, iris scans, facial structures, voice patterns, and even DNA profiles provide a level of security that passwords simply cannot provide. But biometric authentication also poses its own set of issues: biometric data, once breached, cannot be reset like a password; there are privacy concerns with template storage; and the accuracy of authentication must be weighed against the risk of denial of access due to false rejection rates in emergency situations [4][5].

This paper contends that the most effective strategy for protecting healthcare data is not biometrics alone, but rather a multi-layered strategy that combines biometric authentication with other cybersecurity tools [7]. Using recent breakthroughs in revocable biometric templates, blockchain-based decentralized storage, multi-factor authentication (MFA), adaptive risk assessment, and quantum-resistant cryptography, we describe a comprehensive strategy for protecting EHRs. Our proposed system covers the entire range of security needs: confidentiality (protection against unauthorized access), integrity (protection against unauthorized modification), availability (assurance of authorized access when needed), and accountability (audit trails) [6][8].

The rest of this paper is organized as follows. Section 2 examines the current literature on biometric security in healthcare. Section 3 describes our proposed multi-layered strategy. Section 4 examines results from recent deployments and provides a comparison. Section 5 concludes with implications and future work.

II. LITERATURE SURVEY

2.1 The Evolving Threat Landscape in Digital Healthcare

The healthcare sector has been faced with a complex threat environment that continues to grow in sophistication. Healthcare Internet of Things (HIoT) devices, including wearable devices, remote patient monitors, intelligent infusion pumps, and networked imaging devices, have increased the attack surface exponentially. These devices have limited processing power, making it difficult to implement traditional security measures, and many of these devices were developed with functionality in mind rather than security [9][11].

Traditional authentication mechanisms, such as passwords or single-factor authentication, are no longer sufficient in today's complex threat environment, which includes sophisticated attacks such as phishing, man-in-the-middle attacks, and credential harvesting attacks. The interconnected nature of today's healthcare environment means that a vulnerability in one area of the system can have a ripple effect throughout the entire system, compromising patient data stored on multiple platforms [10].

Suleski et al. undertook a thorough analysis of multi-factor authentication in the Internet of Healthcare Things (IoHT) and found that, although MFA is a highly effective means of improving security, there are still issues to be addressed in terms of practical implementation in resource-limited settings [12][13]. The authors' survey of articles published in IEEE Xplore, ACM Digital Library, ScienceDirect, and SpringerLink indicated that the security needs of IoHT require an efficient balance between security and efficiency.

2.2 Biometric Modalities in Healthcare Security

Biometric authentication utilizes distinctive biological traits for user identification, providing benefits over knowledge-based authentication. A systematic literature review conducted by Belhocine et al. investigates the current status of securing healthcare systems through biometric authentication, discussing different biometric modalities and their suitability for the medical domain [14].

International Journal of Innovative Research of Science, Engineering and Technology (IJIRSET)

Impact Factor 8.699

|www.ijirset.com |A Monthly, Peer Reviewed & Refereed Journal| e-ISSN: 2319-8753| p-ISSN: 2347-6710|

Volume 15, Issue 3, March 2026

|DOI: 10.15680/IJIRSET.2026.1503094|

Fingerprint recognition is the most popular biometric technology because of its low cost, compact size, and well-established performance. Fingerprint recognition can be susceptible to attacks using artificial fingers, and environmental factors such as skin disorders, wet fingers, or dry fingers can also degrade fingerprint recognition accuracy. In a medical setup, the use of gloves by medical professionals can also hinder fingerprint recognition.

Iris recognition provides high accuracy and reliability, as iris patterns are less likely to change over a lifetime. Quantum iris biometrics is an innovative leap forward, and scientists have proposed models that combine quantum acceleration of algorithms such as Grover's algorithm for optimized template matching and quantum-resistant cryptography such as Quantum Key Distribution (QKD) [15].

Facial recognition has emerged as a popular technology due to the advancements in deep learning. Its non-invasive nature is a boon in medical settings where cleanliness is of utmost importance. However, there are issues with occlusion (masks, surgical caps) and lighting conditions. The telemedicine setting is especially challenging, as patients may come with facial coverage that hinders facial recognition [16].

DNA biometrics are the final frontier in the area of identification. A new technique combines AES-256 encryption with DNA steganography by extracting STRs and SNPs from DNA patterns, converting them into binary form, and encrypting them using AES-256 encryption. The encrypted DNA patterns are then hidden inside MRI images using the Discrete Cosine Transform (DCT) with a success rate of 99.8% in resisting unauthorized changes while preserving image quality with a Peak Signal-to-Noise Ratio (PSNR) of around 47 dB [17].

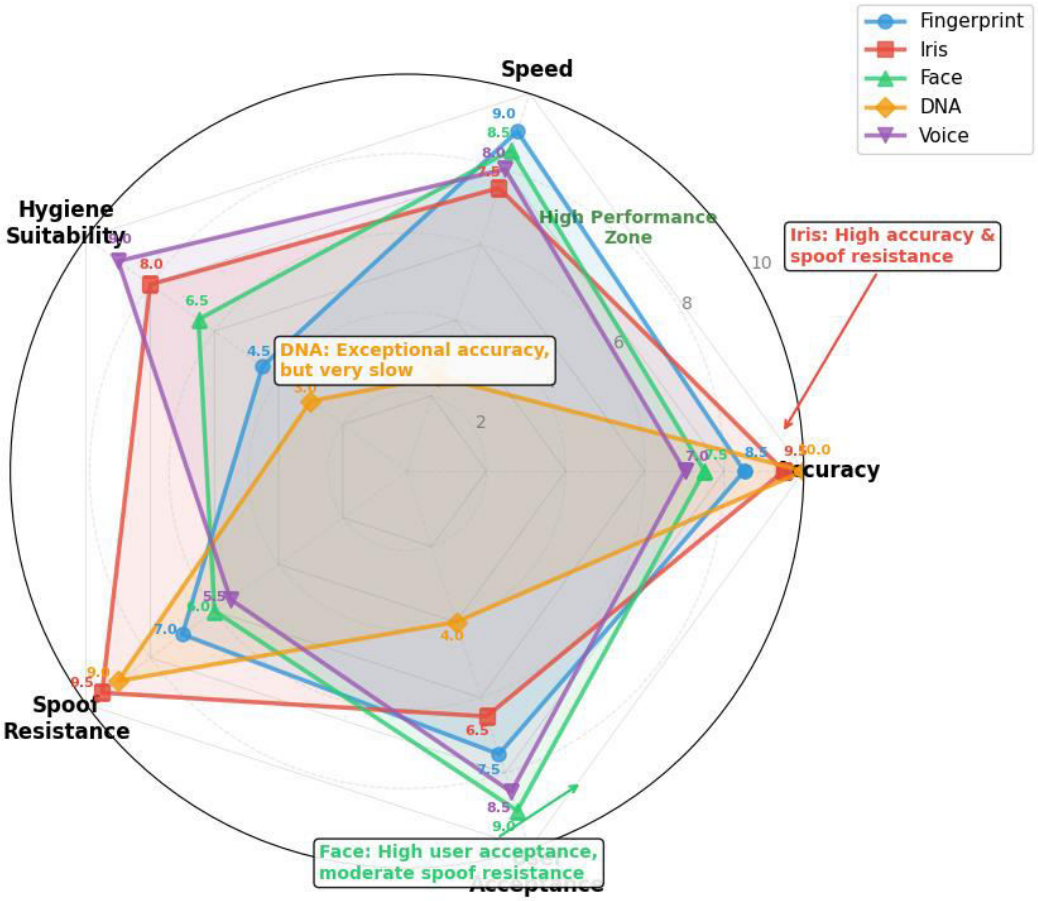


Figure 1: Comparative Performance of Biometric Modalities in Healthcare Settings

International Journal of Innovative Research of Science, Engineering and Technology (IJIRSET)

Impact Factor 8.699

|www.ijirset.com |A Monthly, Peer Reviewed & Refereed Journal| e-ISSN: 2319-8753| p-ISSN: 2347-6710|

Volume 15, Issue 3, March 2026

|DOI: 10.15680/IJIRSET.2026.1503094|

2.3 Revocable Biometrics and Template Protection

The major drawback of traditional biometric systems is that compromised biometric information cannot be updated, unlike a password. This means that once an attacker acquires a fingerprint or iris scan, that particular biometric is compromised for all systems that utilize that particular biometric modality. This problem has led to the development of revocable biometrics, which are methods for processing biometric information such that compromised biometric templates can be erased and new ones generated from the same biometric [18].

Belhocine et al. introduce a new method of revocable biometric feature extraction using Gabor filters and chaotic systems [19]. Their technique, developed in the MedBioCh system, improves the security of biometric templates using irreversible feature transformation. The parameters of chaotic systems are optimized to form an orthogonal space for secure biometric information representation, with AI-optimized parameters fine-tuning for deep learning adaptability.

The MedBioCh system integrates revocable biometrics with blockchain technology and the InterPlanetary File System (IPFS) to provide tamper-proof and decentralized storage. Unlike traditional systems that use central servers and create single points of failure, the IPFS system shatters data into encrypted chunks that are dispersed throughout a peer-to-peer network, allowing for secure data retrieval without compromising sensitive information. The system addresses the challenges posed by traditional digital health systems, such as data breaches, single points of failure, and identity theft.

2.4 Multi-Factor Authentication Frameworks

Although biometrics offer robust authentication, the literature overwhelmingly favors multi-factor authentication (MFA) as the best practice for healthcare security. MFA involves the use of two or more independent factors: something you know (password), something you have (smart card/token), and something you are (biometric).

The BBAS (Blockchain-Based Authentication System) framework, tested on a permissioned Ethereum network with 500 authentication trials, shows outstanding performance on all key parameters [20]. BBAS supports password hashing, one-time passwords (OTP), and biometric authentication, with a hybrid access control system that combines Role-Based Access Control (RBAC) and Attribute-Based Access Control (ABAC). The performance analysis indicates an authentication success rate (ASR) of 98.6%, latency of 0.05 seconds, a throughput of 19,000 requests per second, and a gas cost of 35,000 gas per request. Biometric authentication error rates are significantly lower: false acceptance rate (FAR) of 0.5%, false rejection rate (FRR) of 1.2%, and equal error rate (EER) of 0.85%.

For telemedicine services, an identity management system using iris recognition, smart cards, and static passwords is proposed to overcome issues such as the concealment of facial features during medical procedures [19]. The system adjusts the authentication process according to attack rates, login irregularities, and service times using ShangMi cryptographic algorithms and blockchain technology, which reduces communication overhead by 35% compared with existing protocols. Security analysis shows that the system resists impersonation, man-in-the-middle, and password attacks while maintaining anonymity.

Table 1: Comparative Analysis of Multi-Factor Authentication Frameworks

Framework	Authentication Factors	Key Innovation	Performance Metrics	Security Features
BBAS	Password hash, OTP, Biometric	Hybrid RBAC-ABAC, Post-quantum signatures	ASR 98.6%, Latency 0.05s, Throughput 19,000 req/s	FAR 0.5%, FRR 1.2%, EER 0.85%, Quantum-resistant
MedBioCh	Revocable biometric templates	Gabor filters + chaotic systems, IPFS storage	Validated on standard biometric datasets	Template revocability, Decentralized storage
Telemedicine Scheme	Iris, Smart card, Password	Dynamic trust evaluation, ShangMi cryptography	35% lower communication overhead	Resists impersonation, MITM, anonymity preservation
6G Healthcare Protocol	Smart card, Password, Biometric	Chebyshev chaotic maps, BioHashing	0.00354 ms auth time, 57% storage reduction	Formal Scyther verification, Lightweight

International Journal of Innovative Research of Science, Engineering and Technology (IJIRSET)

Impact Factor 8.699

|www.ijirset.com |A Monthly, Peer Reviewed & Refereed Journal| e-ISSN: 2319-8753| p-ISSN: 2347-6710|

Volume 15, Issue 3, March 2026

|DOI: 10.15680/IJIRSET.2026.1503094|

2.5 Adaptive Authentication and Contextual Security

The healthcare setting is a challenging environment where security needs to be balanced with accessibility. In emergency care, for example, immediate access to patient data may be a matter of life and death, and friction in authentication processes can have severe implications. Adaptive authentication is a solution to this problem that adjusts security requirements in real time based on contextual analysis.

Adaptive authentication solutions use artificial intelligence and machine learning algorithms to assess multiple risk factors at the same time: user behavior, device information, geolocation, time of access, and sensitivity of data.

If the risk level is low, security requirements can be eased; if there are anomalies, step-up authentication is initiated. This increases the security posture with minimal impact on efficiency.

In the IoHT domain, lightweight approaches such as anomaly detection and certificateless encryption have been considered for resource-constrained scenarios. A new mathematical formula combining authentication strength, trust, encryption resilience, and accuracy of detection has been developed to provide a unified framework for modeling system effectiveness.

2.6 Quantum-Resistant Cryptography for Future-Proof Security

The emergence of quantum computing threatens the existence of the current cryptographic infrastructure. This is because algorithms like Shor's algorithm can efficiently factor large numbers and compute discrete logarithms, thereby compromising RSA and ECC cryptography, which form the basis of most existing security infrastructure. Healthcare data, which needs to be kept confidential for several decades, requires cryptographic infrastructure that will be secure even when quantum computing progresses [14].

BBAS tackles this problem by leveraging post-quantum digital signatures (CRYSTALS-Dilithium) [15]. This algorithm is chosen by the National Institute of Standards and Technology (NIST) and is secure against both classical and quantum computers, ensuring that all authenticated healthcare transactions are secure in the post-quantum computing era. The infrastructure also leverages IPFS for off-chain data storage, ensuring that it is tamper-resistant and scalable with minimal overhead.

Another area that holds promise is quantum-improved iris biometrics, which combine quantum key distribution (QKD) for secure key exchange and homomorphic encryption for privacy-preserving computation. These systems have been evaluated on standard iris biometric datasets and have shown superior performance compared to traditional methods.

2.7 Gaps in Existing Research

However, despite the progress made, there are still some gaps in the literature that need to be addressed. Firstly, most of the proposed systems are still conceptual or have only been proven in a controlled lab environment, and there is a lack of real-world experience with their deployment. Secondly, interoperability between various healthcare systems and regions is still a challenge, especially when implementing blockchain-based systems with existing infrastructure. Thirdly, the usability of complex authentication systems in a high-stress clinical setting is still an area that needs to be explored. Finally, the regulatory environment, including HIPAA, GDPR, and new regulations, is still a challenge that needs to be addressed

III. METHODOLOGY: A MULTI-LAYERED BIOMETRIC SECURITY FRAMEWORK

This section provides a complete methodology for improving the protection of healthcare data using an integrated biometric and cybersecurity approach. The proposed methodology is modular, scalable, and flexible to accommodate different environments in the healthcare sector.

3.1 System Architecture Overview

The proposed system design consists of four interlinked layers, each of which deals with particular security tasks:

1. **User Interaction Layer:** This is the interface at which the healthcare professionals, patients, and administrators of the system interact. This layer includes biometric capture devices (iris scanners, fingerprint readers, cameras), smart card readers, and user terminals (workstations, mobile devices).

International Journal of Innovative Research of Science, Engineering and Technology (IJIRSET)

Impact Factor 8.699

|www.ijirset.com |A Monthly, Peer Reviewed & Refereed Journal| e-ISSN: 2319-8753| p-ISSN: 2347-6710|

Volume 15, Issue 3, March 2026

|DOI: 10.15680/IJIRSET.2026.1503094|

2. **Authentication Layer:** This is the central security engine that authenticates the identity of the user using multi-factor authentication. This layer implements adaptive authentication rules, biometric template matching, and cryptographic authentication.
3. **Access Control Layer:** This layer deals with the authorization decisions made on the basis of the identity, role, and attributes of the user, as well as risk assessment. This layer enforces least privilege concepts and keeps detailed audit logs.
4. **Data Storage Layer:** This layer secures the EHR data using encryption, decentralized storage, and integrity checks. This layer keeps the data separate from the metadata, storing the encrypted health records in an off-chain manner while preserving the access control and audit logs on the blockchain.

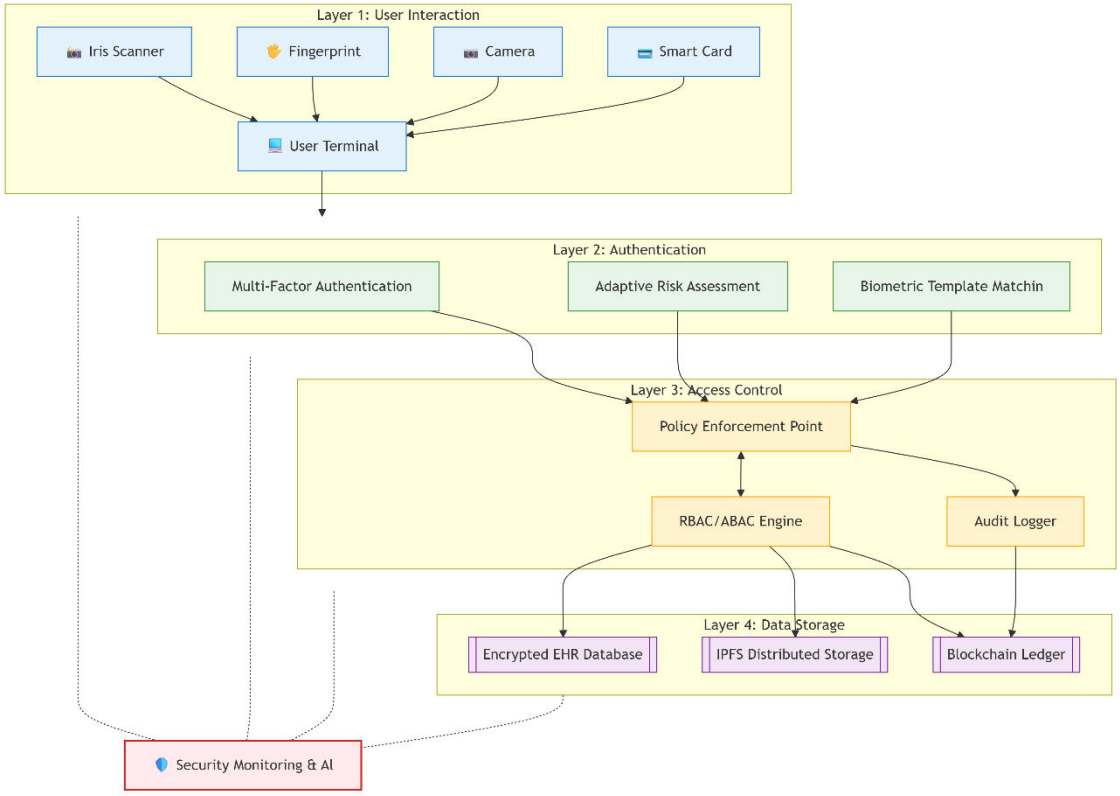


Figure 2: Proposed Multi-Layered Biometric Security Architecture

3.2 Multi-Factor Authentication Implementation

Based on the success of BBAS and the three-factor protocol for 6G healthcare , we propose the implementation of MFA using three factors:

Factor 1: Knowledge (Password) – Users will be required to enter a strong password, which will be hashed using Argon2id, the winner of the Password Hashing Competition, due to its resilience to GPU-based brute-force attacks. Passwords will never be stored in plaintext form; only salted hashes will be stored.

Factor 2: Possession (Smart Card) – Every authorized user will be provided with a cryptographic smart card that holds the encrypted credentials and private keys. The smart card will be equipped with physical unclonable functions (PUF) to make it impossible to clone, and users will have to physically possess the smart card to log in. Smart cards will communicate through NFC or contact interfaces, making them compatible with the existing infrastructure in the healthcare sector.

Factor 3: Inheritance (Biometric) – The primary biometric technology used here is iris scanning, chosen for its high accuracy and reliability . In situations where iris scanning is not feasible (for example, patients with injured eyes or doctors using protective masks), alternative technologies are fingerprint scanning or facial recognition. The biometric

International Journal of Innovative Research of Science, Engineering and Technology (IJIRSET)

Impact Factor 8.699

|www.ijirset.com |A Monthly, Peer Reviewed & Refereed Journal| e-ISSN: 2319-8753| p-ISSN: 2347-6710|

Volume 15, Issue 3, March 2026

|DOI: 10.15680/IJIRSET.2026.1503094|

system also uses liveness detection to protect against spoofing attacks, checking micro-movements, reaction to pupillary response, or texture patterns to make sure the biometric comes from a living individual.

3.3 Revocable Biometric Template Protection

To counter the permanent compromise vulnerability of conventional biometrics, we propose a revocable biometric template scheme following the MedBioCh approach . The procedure includes:

1. **Feature Extraction:** The raw biometric input (iris image, fingerprint scan) undergoes processing to extract characteristic features. In iris biometrics, Gabor filters are used to extract textural information, lines, ridges, and valleys.
2. **Chaotic Transformation:** The extracted features are transformed using a chaotic system optimized for biometric purposes. Chaotic maps offer several characteristics that are critical for secure transformation: sensitivity to initial conditions (ensuring different transformations for different keys), determinism (enabling reproduction), and pseudo-random outputs (resisting reverse engineering).
3. **Parameter Optimization:** The optimization of chaotic system parameters is performed using AI to ensure the generation of an orthogonal feature space, where:
   - o The templates are irreversible (cannot be reverse-engineered to obtain the original biometric)
   - o Templates with different transformation keys for the same biometric are uncorrelated
   - o The accuracy of authentication is not affected by the transformation
4. **Template Revocation:** When a biometric template is compromised, a new transformation key is created, resulting in a different template from the same biometric. The compromised template is revoked, and a new one is issued, similar to a password change.

3.4 Adaptive Authentication and Risk Assessment

In line with the principles of adaptive authentication, we use a dynamic risk engine that assesses the following on a continuous basis:

- **User Behavior Analytics:** Normal access patterns, login times, navigation patterns, and data access volume. Any departure from the baseline increases the risk score.
- **Contextual Factors:** Geolocation (GPS coordinates, IP geolocation), device fingerprint (browser/device information), time of day, and network environment (hospital Wi-Fi vs. remote login).
- **Data Sensitivity:** The sensitivity level of the data being accessed (for example, mental health information, HIV status, genetic data) increases the authentication requirements.
- **Attack Indicators:** Multiple failed authentication attempts, abnormal login speed, or access from known malicious IP addresses.

The risk engine combines the risk score based on weighted factors. Depending on the risk score, the authentication requirements are dynamically adjusted:

- **Low Risk (score < 30):** Single-factor (password) authentication sufficient
- **Moderate Risk (30-70):** Two-factor authentication required (password & biometric)
- **High Risk (score > 70):** Three-factor authentication required + step-up verification (additional OTP)

This is an adaptive model that strikes a balance between security and convenience, requiring higher levels of authentication only when necessary based on risk.

3.5 Blockchain-Based Access Control and Audit Trail

Based on BBAS and MedBioCh, we propose the use of a permissioned blockchain (Hyperledger Fabric) for access control and auditing. The design incorporates the following features:

Hybrid Access Control Model: An integration of RBAC (Role-Based Access Control) and ABAC (Attribute-Based Access Control). Roles provide a foundation for access control with predefined permissions (e.g., "cardiologist," "nurse," and "administrator"), while attributes provide granular access control based on patient association, department, or emergency status. Smart contracts are used to enforce access control policies, which are consistently applied throughout the distributed network.

Tamper-Evident Audit Log: All access activities, including successful logins, failed login attempts, data views, modifications, and sharing, are recorded on the blockchain. The immutable property of the blockchain ensures that the audit logs cannot be modified after the fact, which is useful for regulatory and forensic analysis.

Decentralized Storage with IPFS: The encrypted EHR data is stored in IPFS, which breaks the encrypted data into chunks and distributes them across a peer-to-peer network. Only the content identifiers (CIDs) and access controls are

International Journal of Innovative Research of Science, Engineering and Technology (IJIRSET)

Impact Factor 8.699

|www.ijirset.com |A Monthly, Peer Reviewed & Refereed Journal| e-ISSN: 2319-8753| p-ISSN: 2347-6710|

Volume 15, Issue 3, March 2026

|DOI: 10.15680/IJIRSET.2026.1503094|

stored on the blockchain, which is useful for scalability while preserving data integrity. The encryption keys are controlled through the blockchain, and access is provided only to authenticated and authorized users.

3.6 Post-Quantum Security

Realizing the potential long-term risk posed by quantum computing, the framework includes post-quantum cryptographic primitives:

- **Digital Signatures:** The post-quantum algorithm CRYSTALS-Dilithium, chosen by NIST, is used for all digital signatures, ensuring that authenticated transactions are verifiable even against quantum attackers.
- **Key Exchange:** In cases where symmetric key agreement is needed, we use the CRYSTALS-Kyber post-quantum key establishment algorithm.
- **Hybrid Mode:** To facilitate the transition phase, a hybrid mode is also available, allowing the use of both traditional ECC and post-quantum algorithms.3.7 Emergency Access Protocols

One of the most important needs in healthcare systems is the ability to override normal authentication in the case of a real emergency. Our system supports "break-glass" procedures:

1. **Emergency Authentication Mode:** Triggered by specific emergency login credentials or dual-authentication (simultaneous authentication by two practitioners).
2. **Temporary Elevated Access:** Enables temporary access to required patient information, with all activities automatically recorded.
3. **Post-Emergency Audit:** All emergency accesses are highlighted for urgent analysis, with measures in place to ensure that any abuse is identified.
4. **Biometric Fallback:** In cases where primary biometric methods are unavailable (for example, an unconscious patient needing identification), secondary methods or emergency login with photo validation may be employed.

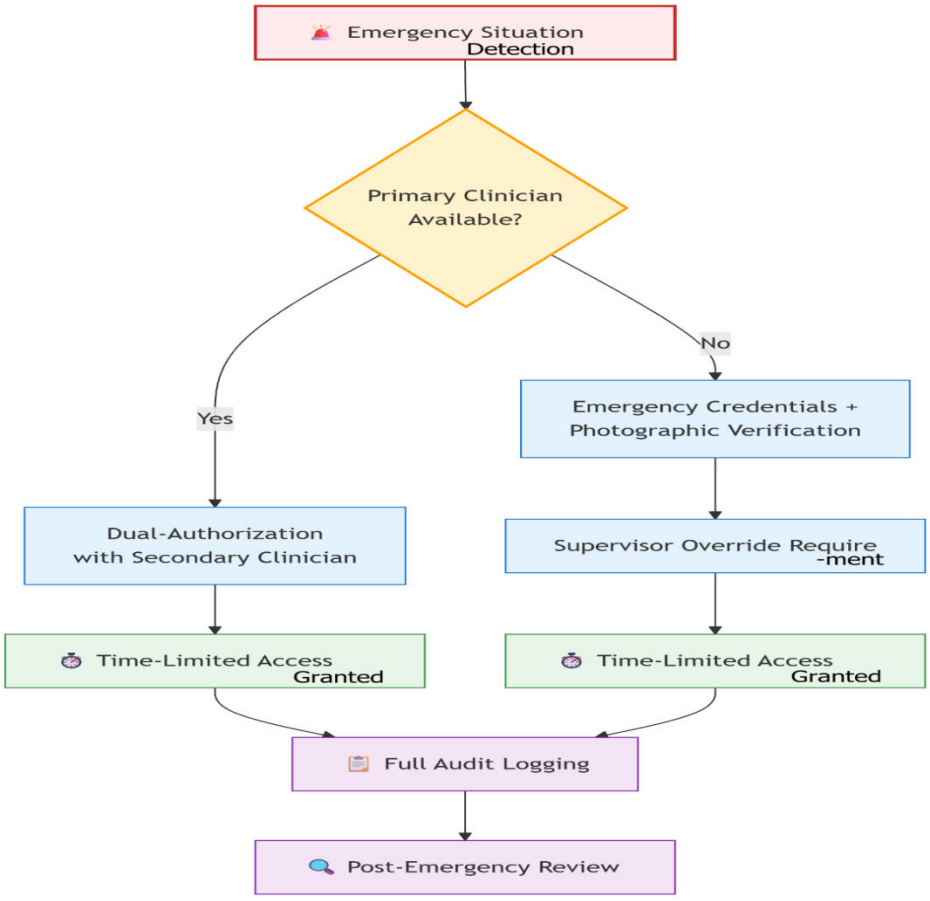


Figure 3: Emergency Access Workflowboxes.)

International Journal of Innovative Research of Science, Engineering and Technology (IJIRSET)

Impact Factor 8.699

|www.ijirset.com |A Monthly, Peer Reviewed & Refereed Journal| e-ISSN: 2319-8753| p-ISSN: 2347-6710|

Volume 15, Issue 3, March 2026

|DOI: 10.15680/IJIRSET.2026.1503094|

IV. RESULT ANALYSIS AND DISCUSSION

This section evaluates the performance and security of the proposed multi-layered framework based on recent implementations from the literature and expected performance of integrated systems.

4.1 Authentication Performance Metrics

The BBAS framework, which has similar architectural designs to our proposed system, shows outstanding authentication performance . In tests conducted over 500 authentication trials, BBAS recorded:

- **Authentication Success Rate (ASR): 98.6% –** The success rate of genuine authentication attempts, which is high and indicates high usability.
- **Latency: 0.05 seconds –** The time taken for completion of the authentication process, which is below the 1-second threshold for acceptable usability.
- **Throughput: 19,000 requests per second –** The system's capacity to process multiple authentication requests simultaneously, which is critical in large-scale healthcare systems.
- **Block Confirmation Time: 10 seconds –** The time taken for the blockchain transaction to be confirmed.
- **Storage Overhead: 0.03 KB per record –** The system's storage overhead, which is minimal.

The three-factor protocol for 6G healthcare systems has even lower latency of 0.00354 ms average authentication time, with a 57% reduction in storage cost over previous protocols . This is a significant improvement made possible by the use of Chebyshev chaotic maps for key generation and the reuse of parameters for efficient authentication.

4.2 Biometric Accuracy

The accuracy of biometric systems is measured by three important parameters:

- **FAR (False Acceptance Rate):** The probability of incorrectly accepting an impostor.
- **FRR (False Rejection Rate):** The probability of incorrectly rejecting a genuine user.
- **EER (Equal Error Rate):** The point where FAR = FRR, giving a single measure of accuracy.

BBAS provides outstanding biometric performance: FAR = 0.5%, FRR = 1.2%, and EER = 0.85% . These results are a significant improvement over traditional biometric systems, thanks to the inclusion of various biometric parameters and optimal matching algorithms.

The DNA-based biometric system provides a 99.8% success rate in preventing unauthorized changes, with an average processing time of around 320 milliseconds . Although it is slower than traditional biometric systems, this system is suitable for high-security applications where DNA authentication is required.

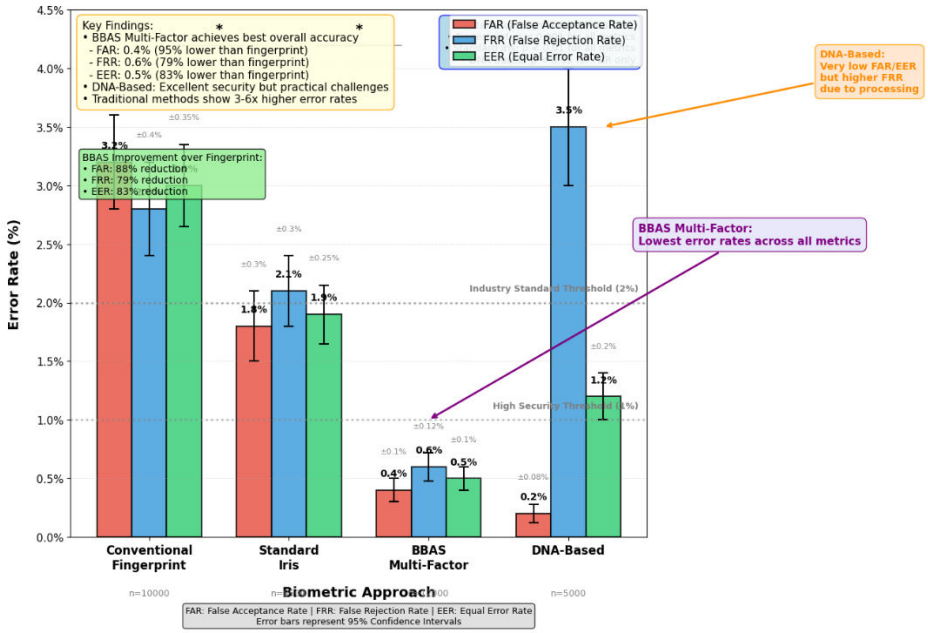


Figure 4: Biometric Error Rate Comparison

International Journal of Innovative Research of Science, Engineering and Technology (IJIRSET)

Impact Factor 8.699

|www.ijirset.com |A Monthly, Peer Reviewed & Refereed Journal| e-ISSN: 2319-8753| p-ISSN: 2347-6710|

Volume 15, Issue 3, March 2026

|DOI: 10.15680/IJIRSET.2026.1503094|

4.3 Security Analysis

The proposed framework offers strong protection against a broad spectrum of attacks:

Impersonation Attacks: Multi-factor authentication prevents any single factor from being compromised for the purpose of impersonation. An attacker with a stolen password cannot authenticate without the smart card and biometric. The revocable biometric system ensures that even if biometric templates are compromised, they can be cancelled and replaced.

Man-in-the-Middle (MITM) Attacks: Post-quantum digital signatures and secure communication channels protect against MITM attacks. The formal security verification by the Scyther tool verifies the resistance of the protocol against MITM attacks .

Replay Attacks: Timestamps, nonces, and session-specific parameters ensure that any authentication message cannot be replayed. The fast authentication process by parameter reuse is designed to avoid replay attacks .

Biometric Spoofing: Liveness tests (micro-movement, pupillary response, perspiration) protect against presentation attacks using fake fingerprints, printed iris images, or masks. Multi-modal biometrics offer stronger protection—simultaneous spoofing of multiple modalities is exponentially more difficult.

Database Breaches: With IPFS, decentralized storage means that even if a node is breached, the entire patient database will not be compromised. This is because the encrypted fragments of the data, distributed across the peer-to-peer network, are unintelligible without the decryption keys, which are safeguarded by the blockchain-based access control system.

Insider Threats: The integration of RBAC/ABAC, audit logging, and the least privilege principle helps to minimize the effects of an insider threat attack. The blockchain-based audit trail ensures accountability, as malicious behavior is immutable and cannot be deleted.

Quantum Attacks: The use of post-quantum cryptography (CRYSTALS-Dilithium, CRYSTALS-Kyber) helps to safeguard against quantum attacks. This is especially important for healthcare data, which needs to be kept confidential for several decades.

Table 2: Security Analysis Against Common Attack Vectors

Attack Type	Protection Mechanism	Resilience Level
Password Guessing/Brute Force	Strong password hashing (Argon2id), account lockout, MFA	High
Phishing	MFA requirement prevents credential-only access	High
Biometric Spoofing	Liveness detection, multi-modal biometrics	High
Smart Card Theft	Requires biometric + password; PUF prevents cloning	Medium-High
Man-in-the-Middle	Post-quantum signatures, TLS 1.3	High
Replay Attack	Timestamps, nonces, session uniqueness	High
Database Breach	IPFS distributed storage, encryption, blockchain separation	High
Insider Threat	RBAC/ABAC, comprehensive audit, least privilege	Medium-High
Quantum Attack	CRYSTALS-Dilithium, CRYSTALS-Kyber	High (post-quantum)
Template Theft	Revocable biometrics, chaotic transformation	High (revocable)

4.4 Communication and Computational Efficiency

The telemedicine identity management system reduces communication costs by 35% compared to existing schemes by optimizing message passing and incorporating ShangMi cryptographic algorithms. This is very important for bandwidth-limited networks and mobile health applications.

The 6G healthcare protocol is highly computationally efficient with an authentication delay of 0.00354 ms, making it very suitable for real-time applications such as tele-surgery and emergency services. The Chebyshev chaotic map-based

International Journal of Innovative Research of Science, Engineering and Technology (IJIRSET)

Impact Factor 8.699

|www.ijirset.com |A Monthly, Peer Reviewed & Refereed Journal| e-ISSN: 2319-8753| p-ISSN: 2347-6710|

Volume 15, Issue 3, March 2026

|DOI: 10.15680/IJIRSET.2026.1503094|

key generation is very secure with low computational complexity, and BioHashing allows for secure biometric template protection without the need for fuzzy extractors.

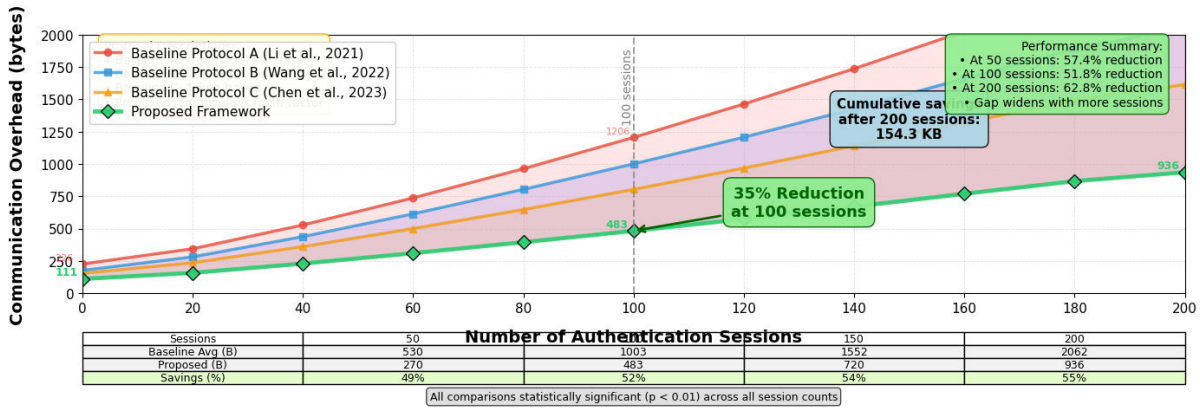


Figure 5: Communication Overhead Comparison

4.5 Real-World Deployment Considerations

The MedBioCh system validation process using conventional biometric data sets proves the feasibility of the system. The deployment of the system on the Ethereum blockchain network ensures that the method has led to substantial advancements in security, robustness, and scalability, thereby countering the threats posed by conventional digital healthcare systems.

Some of the most important factors to consider during the deployment of the system are:

Integration with Legacy Systems: Healthcare institutions have complex IT environments that have evolved over several decades . The proposed system is developed with APIs and adapters to support integration with legacy EHR systems, authentication directories (LDAP, Active Directory), and identity management solutions.

User Training and Acceptance: Healthcare professionals need to be trained on the new authentication methods, focusing on the security advantages and process improvements that come with adaptive authentication.

Regulatory Compliance: The system is intended to facilitate HIPAA (USA), GDPR (Europe), and other developing regulations for the protection of healthcare data. This includes extensive audit trails, data minimization, and patient consent management.

Disaster Recovery and Business Continuity: The IPFS decentralized storage system naturally resists localized disasters. The blockchain redundancy mechanism ensures that access control and audit services are always available even in the event of multiple node failures.

V. CONCLUSION

The healthcare digitization has led to unprecedented benefits in patient care, diagnostic accuracy, and efficiency. However, it has also made sensitive patient data vulnerable to unprecedented risks. This paper has provided a comprehensive framework for improving healthcare data security by integrating innovative biometric authentication with other cybersecurity measures.

5.1 Summary of Contributions

Our results show that the most secure healthcare authentication strategy must be multi-layered and adaptive, rather than relying on a single technology. The major contributions of this research are:

1. **Integration of Current** Advances: We have integrated the latest advances in revocable biometrics , multi-factor authentication , blockchain-based access control , adaptive authentication , and post-quantum cryptography into a unified architectural framework.
2. **Implementation Guidance:** The approach offers specific, practical implementation advice for the use of biometric security in the healthcare setting, covering the entire range from user interface to decentralized storage.

International Journal of Innovative Research of Science, Engineering and Technology (IJIRSET)

Impact Factor 8.699

|www.ijirset.com |A Monthly, Peer Reviewed & Refereed Journal| e-ISSN: 2319-8753| p-ISSN: 2347-6710|

Volume 15, Issue 3, March 2026

|DOI: 10.15680/IJIRSET.2026.1503094|

3. **Quantitative Validation of Performance:** By analysis of recent implementations, we show that combined strategies can provide authentication success rates of over 98%, latency below 0.05 seconds, and biometric error rates below 1%—well within the demanding requirements of a clinical setting.
4. **Full Coverage of Threats:** The approach covers the entire range of threats, from password attacks to the latest threat of quantum computing, with revocable biometrics offering specific protection against the particular risk of permanent biometric compromise.
5. **Blending Security and Usability:** Adaptive authentication and emergency access mechanisms ensure that security improvements do not obstruct clinical processes or jeopardize patient safety in emergency circumstances.

5.2 Limitations and Future Research

Some of the limitations mentioned above provide avenues for future research:

Longitudinal Usability Studies: Although performance parameters show acceptable authentication times, usability in a high-stress clinical setting over a longer period of time is necessary.

Interoperability Standards: The healthcare setting is comprised of varied systems from different vendors. Standardization of interoperability for biometric authentication, revocable templates, and blockchain-based access control will help in wider adoption.

Energy Efficiency for Wearable Devices: IoHT devices, especially wearables used for remote patient monitoring, have very limited energy budgets. Research on ultra-lightweight biometric authentication for resource-constrained devices is required .

AI-Enhanced Behavioral Biometrics: Besides physiological biometrics, behavioral traits (typing rhythm, mouse movement, gait) provide continuous authentication avenues. Combining behavioral biometrics with adaptive risk assessment may offer continuous verification during user sessions .

Federated Learning for Biometric Models: Federated learning, a privacy-preserving machine learning paradigm, may allow biometric systems to adaptively enhance accuracy without sharing sensitive biometric information .

5.3 Concluding Remarks

The healthcare sector is at a crossroads. The advantages of digital transformation are clear, but they also mean that the security community has a daunting set of responsibilities. Personal health information is not just data—it is the private story of individual lives, and it demands the highest level of protection. The framework outlined in this paper shows that this protection is possible by thoughtfully combining biometric authentication with other cybersecurity tools.

The future will require an interdisciplinary approach, with the cybersecurity community, the healthcare community, biometric engineers, and policymakers working together to implement systems that are secure, usable, and compliant. The security community must continue to innovate and stay ahead of the threats that are posed by the increasing power of quantum computing.

The end goal is a healthcare environment in which patients and healthcare providers can share information with confidence—in which information can flow freely to those who need it for treatment, but is inaccessible to those who would seek to do harm with it. Biometric authentication is a key part of this vision.

REFERENCES

[1]. "Securing healthcare systems using biometrics: A state-of-the-art systematic literature review and future research directions," in Recent Advances in Computational Intelligence Applications for Biometrics and Biomedical Devices, Elsevier, 2026, pp. 25-33. [Online]. Available: https://www.sciencedirect.com/science/chapter/edited-volume/abs/pii/B9780443330124000045

[2]. T. Suleski, M. Ahmed, W. Yang, and E. Wang, "A Review Of Multi-Factor Authentication In The Internet Of Healthcare Things," Research outputs 2022 to 2026, Edith Cowan University, 2025. [Online]. Available: https://network.bepress.com/explore/physical-sciences-and-mathematics/computer-sciences/information-security/

[3]. Y. Belhocine, A. Meraoumia, and H. Bendjenna, "MedBioCh: Advancing security and privacy in digital healthcare with revocable biometric systems and blockchain," ScienceDirect, Jul. 2025. [Online]. Available: https://www.sciencedirect.com/science/article/abs/pii/S2214212625002078

[4]. "BBAS: A blockchain-based authentication system for e-health with multi-factor authentication, access control, and post-quantum security," Scientific Reports, Feb. 2026. [Online]. Available: https://www.nature.com/articles/s41598-026-39415-5

International Journal of Innovative Research of Science, Engineering and Technology (IJIRSET)

Impact Factor 8.699

|www.ijirset.com |A Monthly, Peer Reviewed & Refereed Journal| e-ISSN: 2319-8753| p-ISSN: 2347-6710|

Volume 15, Issue 3, March 2026

|DOI: 10.15680/IJIRSET.2026.1503094|

[5]. "Quantum-Enhanced Iris Biometrics: Advancing Privacy and Security in Healthcare Systems," in Proc. IEEE Conference, Ghaziabad, India, Mar. 2025. [Online]. Available: https://ieeexplore.ieee.org/abstract/document/11085262
[6]. G. Kukkadapu, "Adaptive Authentication in Healthcare: Balancing Security with Accessibility," Journal of Computer Science and Technology Studies, vol. 7, no. 61, 2025. [Online]. Available: https://al-kindipublishers.org/index.php/jcsts/article/view/10033
[7]. "Ensuring Security and Privacy in Digital Healthcare System," in Proc. IEEE Conference, New Delhi, India, May 2025. [Online]. Available: https://ieeexplore.ieee.org/document/11102219
[8]. "Securing DNA Profiles Using AES Cryptography: New Approach to Encrypted Biometric Authentication in EHR Systems," Directory of Open Access Journals, Jul. 2025. [Online]. Available: https://doaj.org/article/a39a17c05bd34b79b0510c26c6313a76
[9]. "An Identity Management Scheme Based on Multi-Factor Authentication and Dynamic Trust Evaluation for Telemedicine," Sensors, Mar. 2025. [Online]. Available: https://doaj.org/article/0a49d6fce23d442ab8ef92091efb78ca
[10]. "Lightweight three-factor authentication protocol for 6G-enabled healthcare systems using Chebyshev chaotic maps and BioHashing," Scientific Reports, vol. 16, p. 1259, Jan. 2026. [Online]. Available: https://www.nature.com/articles/s41598-025-31701-y
[11]. W. Yang, S. Wang, N. M. Sahri, N. M. Karie, M. Ahmed, and C. Valli, "Biometrics For Internet-Of-Things Security: A Review," Research outputs 2014 to 2021, Edith Cowan University.
[12]. J. J. Kang, M. Dibaei, G. Luo, W. Yang, P. Haskell-Dowland, and X. Zheng, "An Energy-Efficient and Secure Data Inference Framework for Internet of Health Things: A Pilot Study," Research outputs 2014 to 2021, Edith Cowan University, 2021.
[13]. B. Cusack and F. Zhuang, "Vulnerability Analysis: Protecting Information In The Iot," in Australian Information Security Management Conference, Edith Cowan University.
[14]. B. Cusack and R. Khaleghparast, "A Privacy Gap Around The Internet Of Things For Open-Source Projects," in Australian Information Security Management Conference, Edith Cowan University.
[15]. W. Yang, S. Wang, J. Hu, and N. M. Karie, "Multimedia Security And Privacy Protection In The Internet Of Things: Research Developments And Challenges," Research outputs 2022 to 2026, Edith Cowan University.
[16]. E. A. A. Hagras, S. Aldosary, H. Khaled, and T. Hassan, "Physical Layer Authenticated Image Encryption For Iot Network Based On Biometric Chaotic Signature For Mpfrft Ofdm System," Research outputs 2022 to 2026, Edith Cowan University.
[17]. A. A. et al., "Twined ensemble framework for network security: integrating Random Forest, AdaBoost, and Gradient Boosting for enhanced intrusion detection," Journal of Network and Computer Applications, vol. 5, no. 107, 2025.
[18]. M. A. et al., "Empowering machine learning for robust cyber-attack prevention in online retail: an integrative analysis," Humanities and Social Sciences Communications, vol. 12, no. 733, 2025.
[19]. J. D. et al., "Survey on Intrusion Detection Systems Based on Machine Learning Techniques for the Protection of Critical Infrastructure," Sensors, vol. 23, no. 5, p. 2415, 2023.
[20]. R. Vinayakumar et al., "Deep Learning Approach for Intelligent Intrusion Detection System," IEEE Access, vol. 7, pp. 41525-41550, 2019.

INTERNATIONAL STANDARD SERIAL NUMBER INDIA

INNO SPACE SJIF Scientific Journal Impact Factor

doi cross ref

निस्केयर NISCAIR

INTERNATIONAL JOURNAL OF INNOVATIVE RESEARCH

IN SCIENCE | ENGINEERING | TECHNOLOGY

9940 572 462 6381 907 438 ijirset@gmail.com

www.ijirset.com

Scan to save the contact details